



TITLE: DOCUMENT AUTHENTICATION METHOD AND APPARATUS

BACKGROUND OF THE INVENTION

1. Field of the Invention

5 THIS INVENTION relates to a document authentication method and apparatus.

The invention is particularly suitable for, but not limited to, validation of financial instruments, including cash (ie., bank notes), personal cheques, traveller's cheques, credit cards, debit 10 cards and the like.

The invention is also particularly suitable for, but not limited to, the validation of legal instruments such as letters, agreements, licences, bills, and copies (eg., photocopies) thereof.

2. Prior Art

15 The counterfeiting of documents, particularly currency, has been a major problem for the authorities for many years. Money issuing authorities (eg., Reserve Banks or Mints) have adopted many different methods in an attempt to overcome or minimise counterfeiting of currency and other financial documents, and 20 examples have included features or indicia such as watermarks and holograms. Examples of papers discussing such matters include (1) "Spacial Logic Algorithms Using Basic Morphological, Anologic CNN Operations" (Zarande et al) in "The Proceedings of the 1994 Third

IEEE International Workshop on Cellular Neural Networks and their Applications", Rome, Italy, published in the "International Journal of Circuit Theory and Applications" v 24 n 3 May-Jun 1996, pages 283-300; (2) "Development of Embossed Holograms" (Haines) in "Proceedings of SPIE - The International Society for Optical Engineering", v 2652, 1996, Society of Photo-Optical Instrumentation Engineers, Bellingham, WA, United States of America, pages 45-52; (3) "Performance of Diffraction Grating on a Banknote - The Experience with the Australian Commemorative Note" (Hardwick) in "Proceedings of SPIE - The International Society for Optical Engineering", v 1210, published by The International Society for Optical Engineering, Bellingham, WA, United States of America, pages 20-26; (4) "Optically Variable Devices for use on Bank Notes" (Rolle) in "Proceedings of SPIE - The International Society for Optical Engineering" v 1210, published by the International Society for Optical Engineering, Bellingham, WA, United States of America, pages 14-19; (5) "Evaluation of Security Features for new U.S. Currency" (Church et al) in "Proceedings of SPIE - The International Society for Optical Engineering", v 2659, 1996, Society of Photo Optical Instrumentation Engineers, Bellingham, WA, United States of America, pages 28-36.

Whilst such authentication features or indicia can be placed in bank notes, currency or other financial or legal documents,

there is a need for financial or legal instruments bearing such indicia, to be rapidly and accurately-identified and authenticated.

#### SUMMARY OF THE PRESENT INVENTION

It is an object of the present invention to provide a method where a document (eg., a financial or legal instrument, as hereinbefore described), can be authenticated as either valid, or identified as invalid or counterfeit.

It is a preferred object that the method can be carried out rapidly and accurately.

It is a further preferred object to provide a method which requires minimal hardware requirements.

It is a still further preferred object to provide apparatus for carrying out the method.

Other preferred objects will become apparent from the following description.

In one aspect, the present invention resides in a method for authenticating a document (including, eg., a financial or legal instrument as hereinbefore described) including the steps of:

- a) scanning the document for one or more identifying features and/or indicia;
- b) comparing the scanned features/indicia against stored information in a database identifying the features/indicia as authentic or otherwise; and

c) transmitting a signal confirming whether or not the document is authentic or otherwise.

Preferably, the features/indicia scanned include watermarks, holograms, serial numbers, words, devices, colours (eg., patterns, combinations) or other features or indicia printed on, embossed into, incorporated in, or otherwise forming part of, the document.

Preferably, the database contains one or more features/indicia for comparison by which the authentication of the document may be determined. The document may be authenticated when the features/indicia scanned match the criteria of one or more (but preferably a plurality) of identification components stored in the database.

Preferably, when a document is established to be authentic or otherwise, the signal is transmitted to the location at which the document is scanned to indicate whether or not the document is authentic or otherwise and/or one or more alternative locations, eg., to a security unit.

In a second aspect, the present invention resides in apparatus for authenticating a document (eg., a financial or legal document as hereinbefore described) including:

a terminal operable to scan one or more identifying features or indicia of the document;

a database containing one or more stored identifying features indicative of whether or not the document is authentic or otherwise;

comparator means to compare the scanned  
5 features/indicia with the stored identifying features;

transmission means interconnecting the scanning means and the comparator means; and

indicator means operable to receive a signal from the comparator means to indicate whether or not the document is  
10 authentic or otherwise.

Preferably, the indicator means is provided on the terminal. One or more indicator means may be provided at alternative locations, eg., a bank security unit.

Preferably, the terminal includes scanning means  
15 operable to scan the scanned features/indicia hereinbefore described and means to transport the document past the scanning means.

The scanning means may incorporate one or more scanning heads, each operable to scan one or more features/indicia on the documents.

20 The database may be provided on the central computer which incorporates the comparator means.

The transmission means may incorporate any suitable communication means, eg., telephony, wireless, infra-red, hardware

or the like.

In a third aspect, the present invention resides in an apparatus, as described above, where the scanning means is a scanning head passed over the documents (eg., by hand).

5           In a fourth aspect, the present invention resides in an apparatus for authenticating a document (eg., a financial or legal instrument) including;

a receptacle to receive the document;  
means to scan the document as the document enters the  
10          receptacle;

data transfer means to transfer scanned data from the  
scanning means;

and card means operable to receive the data; so  
arranged that:

15           the document can only be released from the receptacle  
when the card means is placed in, or read by, a card reader  
associated with the receptacle.

#### BRIEF DESCRIPTION OF THE DRAWINGS

To enable the invention to be fully understood, preferred  
20          embodiments will now be described with reference to the  
accompanying drawings, in which:

FIG. 1 is a plan view of a document (eg., bank note) to  
be authenticated;

FIG. 2 is a schematic circuit diagram of a first embodiment of the authentication apparatus;

FIG. 3 is a front view of a terminal for the first embodiment;

5 FIG. 4 is a schematic circuit diagram of the scanner of the terminal of FIG. 3;

FIG. 5 is a schematic diagram of a hand-held scanner operable with the terminal of FIG. 3;

10 FIG. 6 is a schematic diagram of a wallet or note holder of a second embodiment; and

FIG. 7 is a schematic diagram of a scanning wand of a third embodiment.

DETAILED DESCRIPTION OF THE  
PREFERRED EMBODIMENTS

15 FIG. 1 is a plan view of a bank note 10 which is an example of a document to be authenticated by the present invention.

The bank note 10 has the following indicia, any one or more of which can be compared against stored indicia:

20

- a) serial number 11;
- b) words 12;
- c) design (optionally coloured) 13;
- d) hologram 14;
- e) signature 15;

- f) photographic image 16;
- g) watermark (or embossing) 17;
- h) micro dots 18; and
- i) thumb- (or finger-) print 19.

5 In a first embodiment (see FIGS. 2 and 3), the system 100 consists of an end user terminal 110 (with a document scanner 111 and end user connector 112) connected to a main computer or central server unit 120 centre that has a resident database 121. The database structure 121 is to be hereinafter described. The computer 10 120 has an input device 122, central processing unit (CPU) 123 and comparing unit 124, the latter comprising the scanned information (e.g., serial number/signature) with the material stored in the database 121.

The end user terminal 110 can be configured in several 15 different ways. It can be a desktop stand-alone device, that is connected to the system in real time. A portable model is also possible in one application that will enable the operator to be away from the network connection. Another configuration of the end user terminal 110 could be the integration of the terminal into a major 20 piece of business equipment.

The end user terminal document scanner 111 consists of a motorised note tray 117 that is used to draw the note (or document) into and through (or into and out of) the terminal. The

note 10 is passed past a pair of scanning heads 113, 114. The scanning heads 113, 114 are doubled to ensure the note 10 can be read no matter which way the note 10 is inserted. (As shown in dashed lines in FIG. 4, the scanning heads 113, 114 may be spaced so that the note 10 passes between them.) The scanning heads contain a number of integrated components, which allow the note 10 to be scanned in several ways. Incorporated in the terminal scanner 111 is an information processing unit 115. The information is passed through a line terminal device 130, that is appropriate to the type of institution where the equipment is installed, to the computer 120.

The motorised tray 117 for the terminal unit 111 allows the note 10 to be pulled past the scanning heads 113, 114 at, preferably, a constant velocity. The motor drive 116 for the rollers 117a of the tray 112 can be preferably set to an almost infinite number of speeds. A motor control unit 118 is integrated into the information processing unit 115 and relies upon an analog (or digital) control mechanism. (It may be manually set by a control 118a.) The type of currency used, the level of identification required and the need for extra analysis can determine the motor control output.

The two identical scanning heads 113, 114 are provided one on each side of the tray 117. In an alternative embodiment, the, or each scanning head may consist of a scanning head with a calibrateable daylight light source and an integrated circuit 115c

10

embedded into the head to control the colour analysis process. The scanner 111 may be commercially available and the specification will depend upon the ultimate requirement of the colour analysis unit. The output of the scanning heads 113, 114 is fed to the information processing unit 115 where the information is filtered and processed.

The information processing unit (IPU) 115 consists of the main processing unit 115a for the information coming from the scanning unit, and an upgradeable memory module with a "flash memory" (or a ROM) 115b. All of the software for the terminal unit 110 and the network interface unit 115 is embedded in the "flash memory" or ROM 115b. The embedding of the software in the "flash memory" or ROM 115b assists in the maintenance of security of the information and to prevent tampering. Within the IPU 115, a security controller is used to monitor the integrity of the unit by monitoring a system of electronic locks and seals throughout the system. Should the integrity of the system be breached, the unit 115 will transmit a security alarm to the network control site via computer 120.

For applications that take the user away from the normal fixed terminal 110, a portable unit 240 (see FIG. 5) will allow the scanning of discrete amounts of information from a note 10 or other instrument. The portable unit 240 scans the area by the user moving the device over the target area (ie., the note 10) in a constant motion. The information is stored in the unit 240 and compared

11

initially against any information held within an onboard memory. The device 240 can have information downloaded from the system 110 and will normally be used as a first level device used to identify notes or other instruments that require further detailed investigation.

5                 The unit 240 consists of a small scanning head 213 with an integrated light source 214. The information from the scanning head 213 is fed into a cut-down version of the IPU 215. The portable device 240 contains a cut-down version of the colour analysis circuitry and is used to do preliminary analysis of a designated area  
10                 on the note. The IPU 215 includes solid state memory that allows the storage of the information gathered from the scan. This information is processed and compared with the information held in memory within the device. Output to the operator is in the form of three lights 241-243 - "green" 241 for "passed", "yellow" 242 for "unknown" and "red" 243 for a note 10 that is found to match a number in the memory and requires confiscation or other action as appropriate. (With a yellow light 242, the note 10 may require manual checking for authenticity/damage.)  
15

20                 The terminal unit 210 can be integrated into almost all money handling machines and processors 250. These include all types and models of cash drawers 251 or totalisers, all money drop boxes, and the units can also be integrated into most secure money safes. The advantage of the system for money storage is that all of

12

the notes and instruments in the cash storage device 251 can be itemised and accounted for.

The terminal equipment 111 can be locationally separate due to the modular design of the terminal unit 111. This configuration is ideal where the system is located in an area that needs to remove large holdings of cash from close proximity of the public interface.

The terminal unit 111 can be upgraded in steps to include an integrated EFTPOS terminal, allow for the printing of microdot security devices, validation of magnetic swipe cards and smart cards, the automatic compilation of foreign currency and the instant conversion of foreign currency in real time when connected to the international network. Supporting the system can be an add-on system that will allow individuals and companies to print their own cheques from their account and incorporate a number of hidden security features that will be able to be detected through the terminal. These security features may be a mixture of colour and position controlled by a secret embedded algorithm.

The system employs a large distributed database 121 in the central computer 120. The database 121 (for, eg., bank notes) (as a "data vault") may contain bank note numbers/types and files that correspond to its colour analysis profile. This profile is reduced to a number through the use of an algorithm that is a part of the

colour analysis system.

When a note 10 or other instrument is fed into the terminal unit 111, the embedded software first determines the denomination of the note 10 through the first output of the colour analysis unit 115c. The note 10 is then fully scanned via the outputs of the scanning heads 113, 114, and the information is passed to the information processing unit 115. The information processing unit 115 resolves the serial number 11 of the note and requests the note file from the central server unit 120. When this information is received by the terminal 111, the serial numbers 11 are compared and all of the alarm flags are checked. Where the note 10 meets these tests, the note approval light 111a is illuminated. Where a note fails one of the tests, a note alarm light 111b is illuminated and the system activates the video surveillance system 150 to record evidence of the person passing the note. The actual process used in this case will vary depending on the threat and safety profile of the end user.

The software in the terminal unit 111 may be embedded within a "flash memory" or a Read Only Memory (ROM) 115b. The software is preferably written in a 4GL language, or any high level language, and compiled prior to the burning of a ROM or placement in the "flash" memory 115b. This is to allow customisation of the software for each particular site. The software is used to determine the denomination of the note 10 through colour analysis and the

structure of all other features/indicia scanned 11-19. Once the scan is completed, the image file is processed to retrieve the note number and a colour profile number is generated.

In a second embodiment (see FIG. 6), portable wallets 5 310 are designed to enable the safe transit of cash or securities.

The wallet 310 has a scanning head 313 which will record the serial number data 11, via a data writer/reader 316, onto a small retrieval card 314, as the cash 10 is scanned as it enters a storage receptacle 311.

10 The card 314 will be required to either deposit, or retrieve, notes 10 from the wallet 310. This will enable the safe transit and storage of the wallet 310.

15 The note 10 can only be retrieved from the wallet 310 if the card 314 is inserted and the data writer/reader 316 instructs a lock 318 to open a door or access panel 319 to the receptacle 311.

In a third embodiment, a small lipstick sized, portable, rechargeable scanning wand 410 (see FIG. 7) enables designated cash notes 10 to be scanned, for instance, in the hotel room before going out shopping. The serial numbers 11 of the scanned notes 10 20 are scanned via a scanning head 413 and stored on a memory unit 415 stored in the wand 410. If the cash (or a wallet/purse containing the cash) is stolen, the wand has a record of the stolen note(s).

An add-on or integrated system associated with a mobile

phone 430 may be used to transmit the stored serial numbers 11 to the central database computer 120 to allow the serial numbers of the notes to be notified to the authorities, eg., police. The unit can also be used to enable a cheque or cash to be cleared at a remote location 5 (eg., purchasing a car on the week-end with a cheque).

The operation of the database 121 will now be described.

The database 121 for currency/bank notes 10 is established as follows:

10 Notes 10 are scanned into the system at the Mint. The serial number 11 and any microdot (or other) security patterns 12-19 are confirmed and stored as a new masterfile and finally a master note image is recorded. From this master image, a reference colour is set and captured.

15 All legitimate serial numbers 11 of all notes 10 and denominations that have been issued by the Mint are on the database.

If a scanned serial number 11 does not match with a serial number 11 legitimately issued by the Mint, an alarm will be sent 20 to the terminal unit 110 via a light or other type of silent alarm.

If a note 10 is presented to the system that creates an image file outside the tolerances of acceptability, the serial number or the masterfile will be marked and the note 10 will be withdrawn from

circulation when presented at a banking interface.

The system will allow the banks to automatically separate the worn, torn damaged and incomplete notes.

It is envisaged that new types of notes will be created to incorporate new colour encryption devices, colour encrypted watermarks, and microdot 18 colour patterns through 16.7 million colours each tied to the serial number. This mark will, in turn, be able to be used to independently verify the validity of the note offline.

In line with new technologies, the clear hologram window 14 can be used to verify the unique polymer colour to add to the overall analysis of the note. This will mean that any particular note will be able to be independently verified with a number of different and independent tests.

Forging of the note 10 will require:

- 15      a) knowledge of the colour serial number link;
- b) knowledge of the encrypted watermark 17;
- c) the use of the correct polymer blend;
- d) a valid serial number 11 from the Mint.

Cheques can have a colour dot serial number link and a link to the signature. The cheque can also, using this feature, have a unique PIN (personal identification number), which will allow the instant authorisation of the cheque.

For ultra secure company cheques, the cheques can be

made up at the company and specially printed with a microdot pattern that gives an audit trail in the company to the process used to draw the cheque. This will allow cheques to be made up on demand and the machine can code all of the information into the cheque pattern  
5 prior to issue.

Another device that can be used to secure the cheque and can be used for travellers cheques is a thumbprint. This print pad can be a polymer that dries quickly when exposed to air. When the cheque is used, the top is peeled off the square and the print made.  
10 Within a very short time, the print dries and the cheque is presented. The scanner detects the image and compares it against a file entry of allowable prints.

Thumb cheques do not require a signature. It is hard to forge a fingerprint and the person who signs the cheque is secret and  
15 no name needs to be on the cheque. The cheque can be authorised upon presentation to the bank or other financial institution. Security devices can be built into the cheque and if a person is made to validate the cheque under duress, a duress fingerprint can be used. The system will be able to recognise the duress alarm and activate the  
20 security procedures.

Signatures can be unreliable, for instance, after injury or with Parkinsons Syndrome. Using the system, a validated signature file can be automatically updated. Validation can use a mixture of

personal verification and advanced software tools such as fractals and chaos analysis.

Travellers cheques can have serial number and PIN identification, and can also incorporate a duress PIN feature and/or 5 can use the polymer thumbprint devices. A PIN signature can be digitally encrypted into the travellers cheque. Stolen cheques can be easily traced and dishonoured.

The system prevents business from:

1. Theft.

All notes stored on the business premises, as 10 scanned, will be on file. If robbed, the owner only needs to press an alarm code and the details of all of the notes on file are transmitted to the security section of the system and marked immediately as stolen. This information is then passed to all of the relevant authorities.

15 2. Misappropriation.

All scanned notes can be put into a database and the business owner knows with confidence the amount of cash flow through the business in relation to stock held or sold.

3. Theft/Misuse of Cheques (Personal and Travellers).

A client is requested, upon opening an account at 20 a financial institution, to supply:

- a) A PIN (personally selected);
- b) Signature;

c) Finger prints - (i) designated finger for

approval; and (ii) designated finger for alarm.

d) Usual identification documentation.

The PIN, signature and fingerprints are all digitized and  
5 stored in the secure database. Whenever a cheque is presented to a  
terminal, the relevant sections of the captured image are analysed  
and compared to the master files in the relevant databases (eg.,  
fingerprint and signature databases).

In addition, a secure PIN number may be entered into the  
10 terminal allowing instant cheque clearance, much like current plastic  
credit cards.

An additional feature of the EFTPOS type terminal could  
include a small digitizer pad for fingerprint authentication. This could  
either replace the current PIN number authentication or be used as an  
15 added layer of security.

Digital signature comparison to master files could be  
included which compares the signature on the credit card with the  
master file signature as well as comparison with the client created  
signature at the site of cash dispersal.

20 All inconclusive results will be referred to a central  
service centre for attention.

Databases (with ongoing upgrade) can store the  
following information:

20

- a) valid note files - include image and serial numbers;
- b) valid note serial numbers;
- c) stolen/missing note registry (NB: a drug dealer who obtains his cash from various drug dealers could potentially be apprehended as he deposits the cash into his/her account, as much of the cash will probably have been stolen in armed robberies, etc.);
- d) destroyed note registry;
- e) damaged note registry (notes earmarked for removal and destruction);
- f) fingerprint digitized image files;
- g) signature digitized image files;
- h) PIN number client registry.

System uses include:

- a) security - all notes scanned into the system, whether in the till, a cash box, safe or wallet, etc.;
- b) counterfeit detection;
- c) damaged note detection;
- d) identification of money laundering and other illegal currency transactions (once the system comes into general use, individual notes can be tracked).

The proposed system (in one or more embodiments) is designed to enable one or more of the following;

1. Cash, personal cheques and travellers cheques to

be assessed for authenticity at the point of presentation.

2. Cash notes, serial numbers and computer image files to be stored at secure national processing laboratory in addition to a central international centre.

5 3. Cash serial numbers, which enter the system, are compared to master files of authentic serial numbers supplied by the national Mint.

4. Cash serial numbers, which enter the system, are compared to master files of stolen note serial numbers.

10 5. Cash serial numbers, which enter the system, are compared to other note serial numbers currently stored within the system to see if any duplications are present.

15 6. Recording and deleting of note serial numbers as they enter and leave the till at the end user interface. This allows a digital record of cash transactions going through the till, in addition to recording the serial numbers of notes held within the till should a thief occur.

7. Colour and image analysis of presented tender, identifying damaged notes which are then recorded centrally and 20 digitally tagged to allow their removal from circulation at an appropriate location.

8. Appropriate law enforcement agencies to be notified of any stolen or forged notes presented to the system or any

notes stolen from the system.

9. Integration of the system into secure tills, secure cash transportation boxes and safes.

10. Remote cash authentication using either a conventional mobile phone with a specifically designed clip-on scanner, or an integrated mobile phone with built-in scanner. Customers can dial into the national centre, enter a PIN number and then scan the notes at the point of sale.

11. Option of small, lipstick sized optical scanner, which can be manually rolled over the serial number on a cash note. This serial number is compared to stored numbers within the ROM within the device. The device is battery powered and the ROM is upgradeable.

12. The tracking of individual notes as they move throughout the market (once the system has been fully implemented within a nation).

13. Integrated internationally operation centre will notify other national centres and law enforcement agencies (eg., FBI) of stolen or forged foreign currency and notes.

14. Personal and travellers cheques can be cleared by using a personal PIN number as well as a signature upon presentation to the system.

15. Personal cheques presented to the system can be

electronically checked against account balances (in a similar fashion to plastic cash cards).

16. Clients' signatures and/or finger prints can be scanned into the system when an account is opened at a financial institution. This master signature file can then be compared against signatures and/or finger print admitted to the system at a later date upon cheque presentation (the fingerprints can be read in "real time" for the cashing of cheques/access to secure areas).

17. Special cheques to be manufactured, which allow a finger print to be placed on the cheque in place of or in addition to a signature. A region of the cheque can have a peel off cover which reveals a polymer pad which enables a fingerprint to be made. The polymer pad solidifies a few seconds after the peel off cover has been removed. Customers can designate the finger they wish to use and can include an alarm finger. Fingerprints allow a degree of anonymity and allow disabled people (eg., Parkinsonism, etc.) to avoid the signature process.

18. Photocopiers where "secure" documents having identifying features/indicia can only be copied by authorised persons.

19. Photographs/video images can be stored and compared for recognition purposes.

20. All the data can be stored in a central "data vault", where third parties are billed each time they access the data

to check the authentication/recognition of a document, etc.

It will be readily apparent to the skilled addressee that the range of potential applications is limitless.

Various changes and modifications may be made to the 5 embodiments described and illustrated without departing from the present invention.

CLAIMS

1. A method for authenticating a document including the steps of:
  - a) scanning the document for one or more identifying features and/or indicia;
  - b) comparing the scanned features/indicia against stored information in a database identifying the features/indicia as authentic or otherwise; and
  - c) transmitting a signal confirming whether or not the document is authentic or otherwise.
2. A method as claimed in Claim 1 wherein:  
the features/indicia scanned include watermarks, holograms, serial numbers, words, devices, colours, patterns, combinations, or other features or indicia printed on, embossed into, incorporated in, or otherwise forming part of, the document.
3. A method as claimed in Claim 2 wherein:  
the database contains one or more features/indicia for comparison by which the authentication of the document may be determined.
4. A method as claimed in Claim 1 wherein:  
the document is authenticated when the features/indicia scanned match the criteria of one or more identification components stored in the database.

5. A method as claimed in Claim 1 wherein:

when a document is established to be authentic or otherwise, the signal is transmitted to the location at which the document is scanned to indicate whether or not the document is authentic or otherwise and/or to one or more alternative locations.

5 6. An apparatus for authenticating a document including:

a terminal operable to scan one or more identifying features or indicia of the document;

10 a database containing one or more stored identifying features indicative of whether or not the document is authentic or otherwise;

comparator means to compare the scanned features/indicia with the stored identifying features;

15 transmission means interconnecting the scanning means and the comparator means; and

indicator means operable to receive a signal from the comparator means to indicate whether or not the document is authentic or otherwise.

7. Apparatus as claimed in Claim 6 wherein:

20 the indicator means is provided on the terminal, and one or more indicator means are optionally provided at alternative locations, eg., a bank security unit.

8. Apparatus as claimed in Claim 6 wherein:

the terminal includes scanning means operable to scan the scanned features/indicia, and means to transport the document past the scanning means.

9. Apparatus as claimed in Claim 8 wherein:

5 the scanning means incorporates one or more scanning heads, each operable to scan one or more features/indicia on the documents.

10. Apparatus as claimed in Claim 6 wherein:

the database is provided on a central computer which 10 incorporates the comparator means.

11. Apparatus as claimed in Claim 6 wherein:

the transmission means incorporates any suitable communication means, including telephony, wireless, infra-red, hardware or the like.

15 12. Apparatus as claimed in Claim 8 or Claim 9 wherein:

the scanning means is a scanning head passed over the documents by hand.

13. An apparatus for authenticating a document including;

a receptacle to receive the document; 20 means to scan the document as the document enters the receptacle;

data transfer means to transfer scanned data from the scanning means;

and card means operable to receive the data; so  
arranged that:  
the document can only be released from the receptacle  
when the card means is placed in, or read by, a card reader  
5 associated with the receptacle.

1 / 7

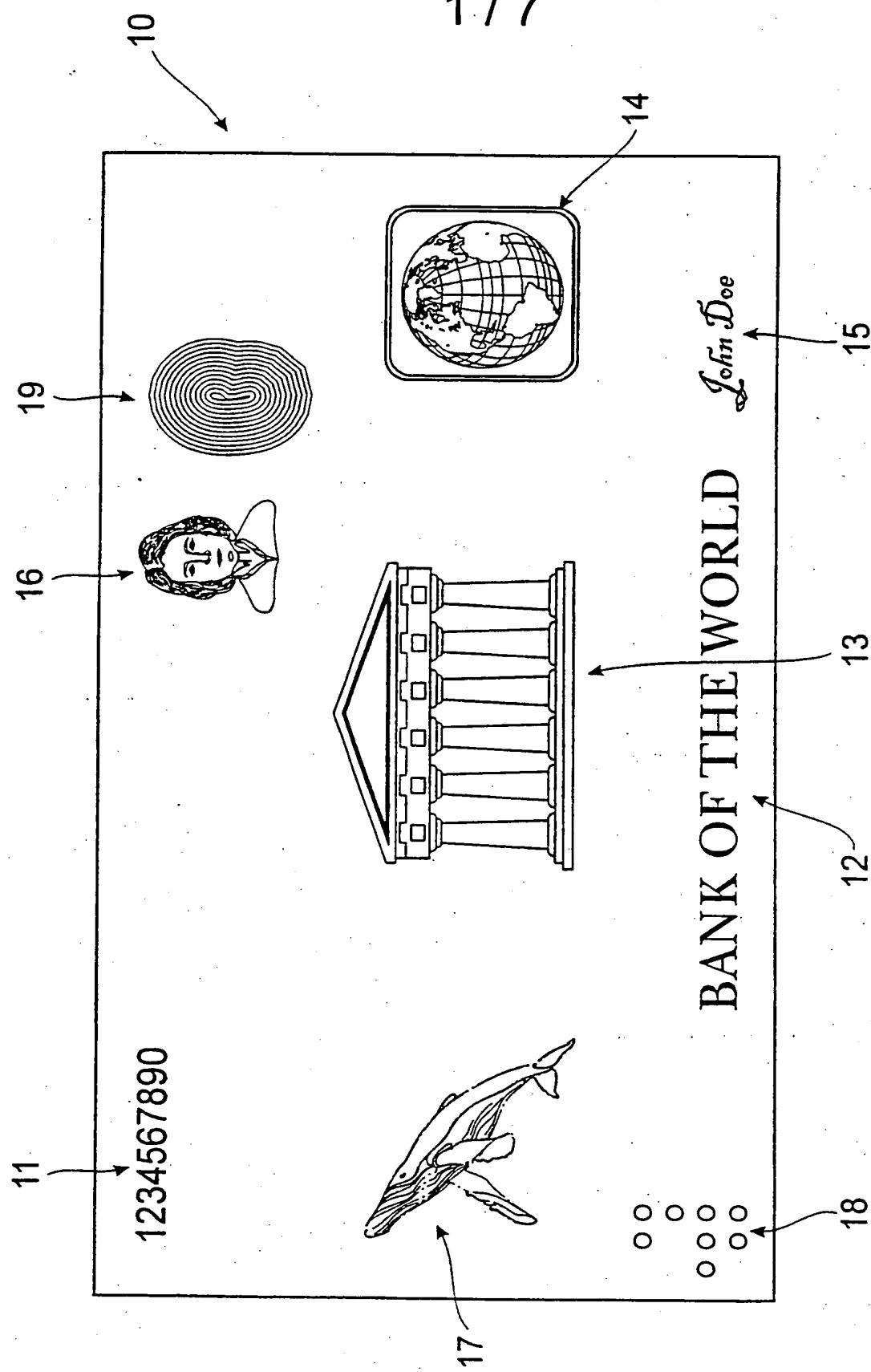


FIG. 1

2 / 7

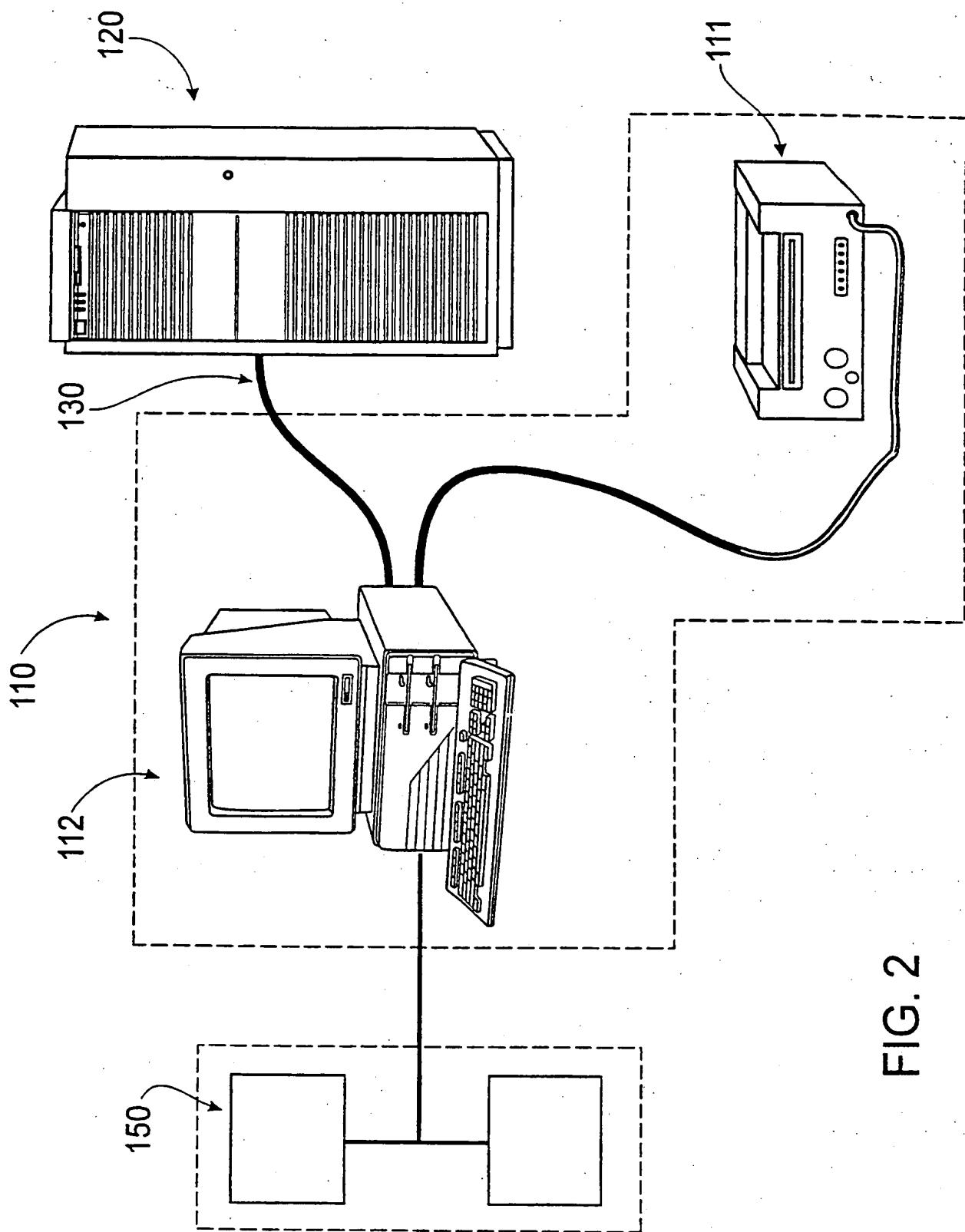


FIG. 2

3 / 7

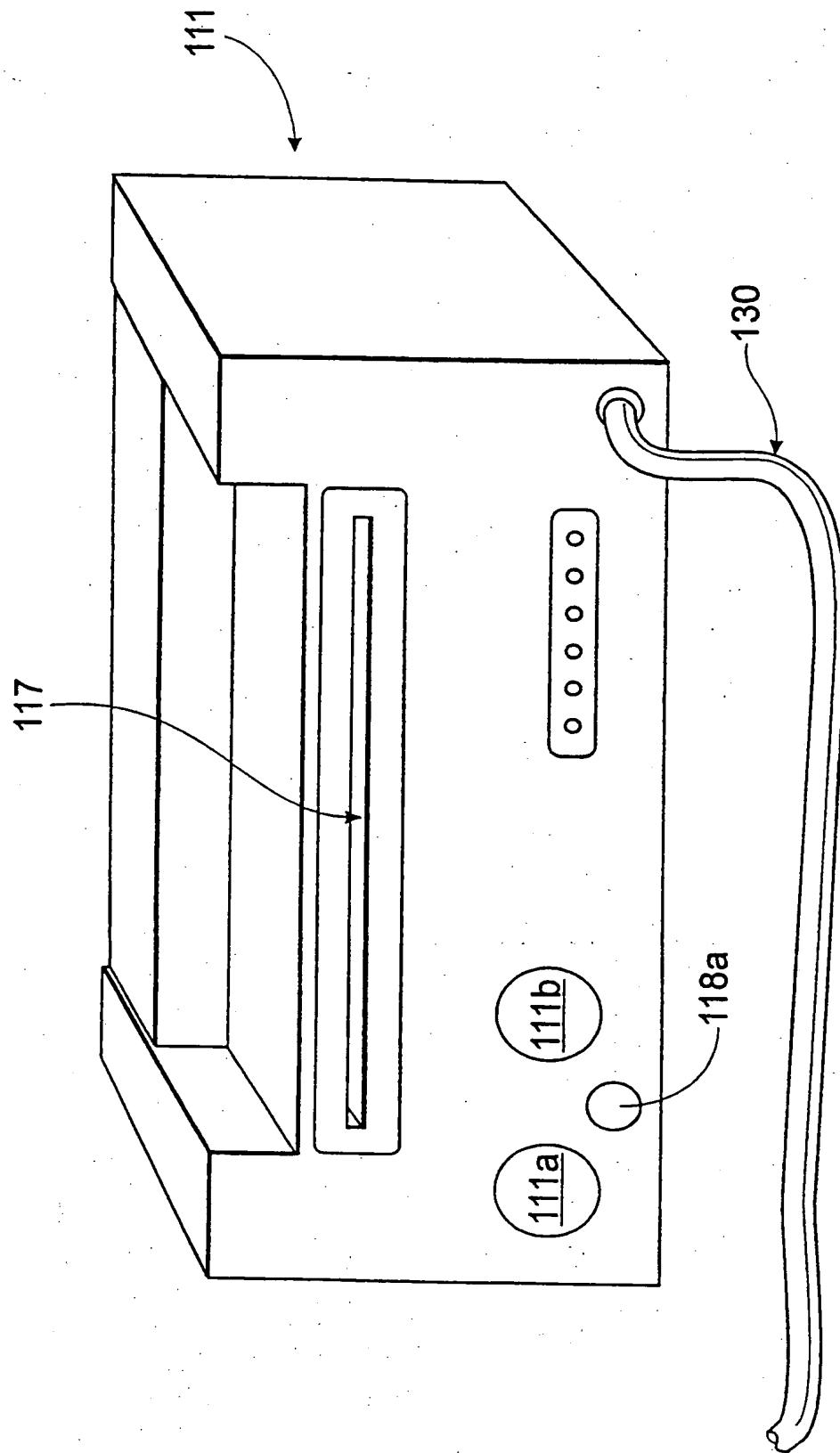


FIG. 3

4 / 7

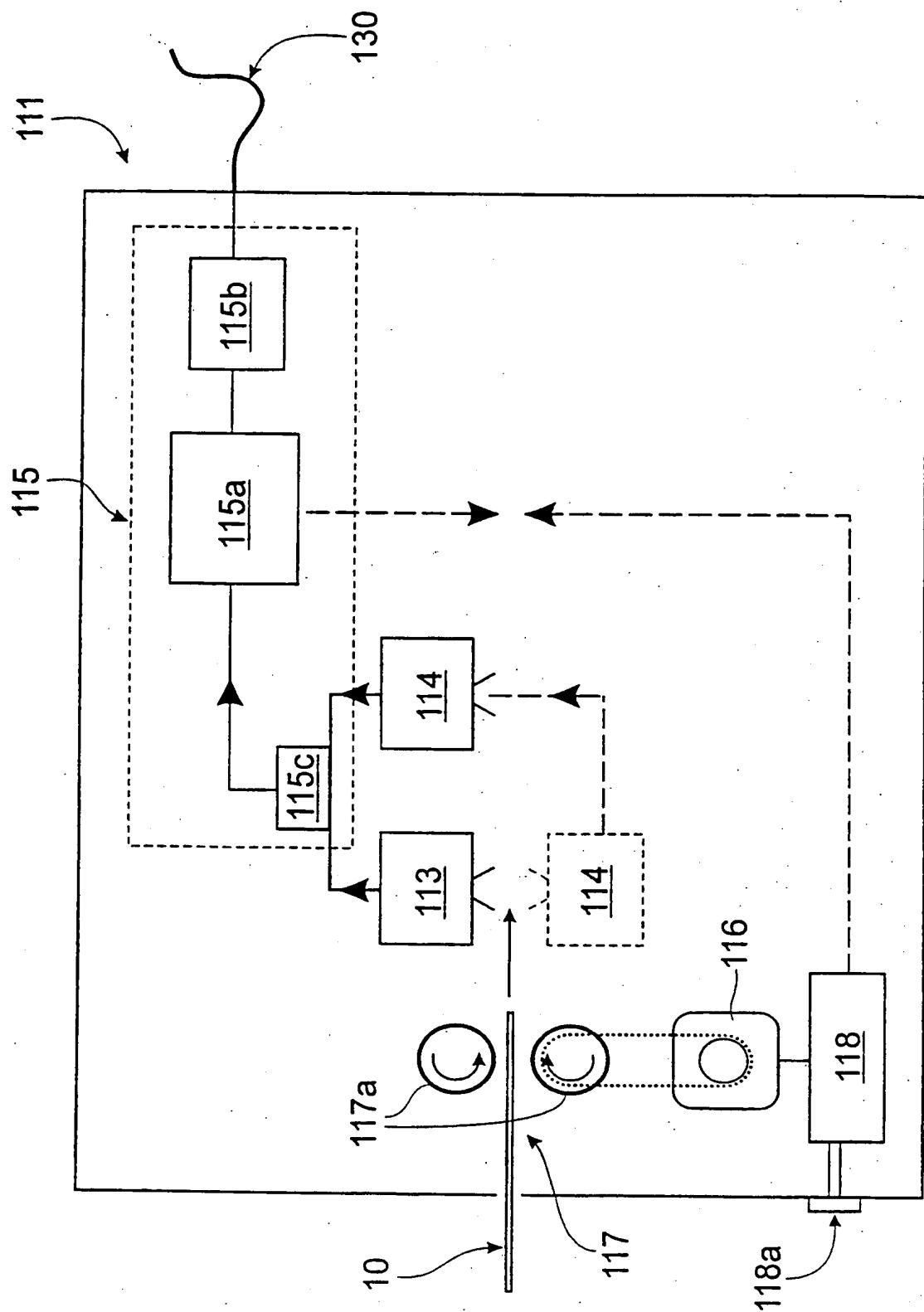


FIG. 4

5 / 7

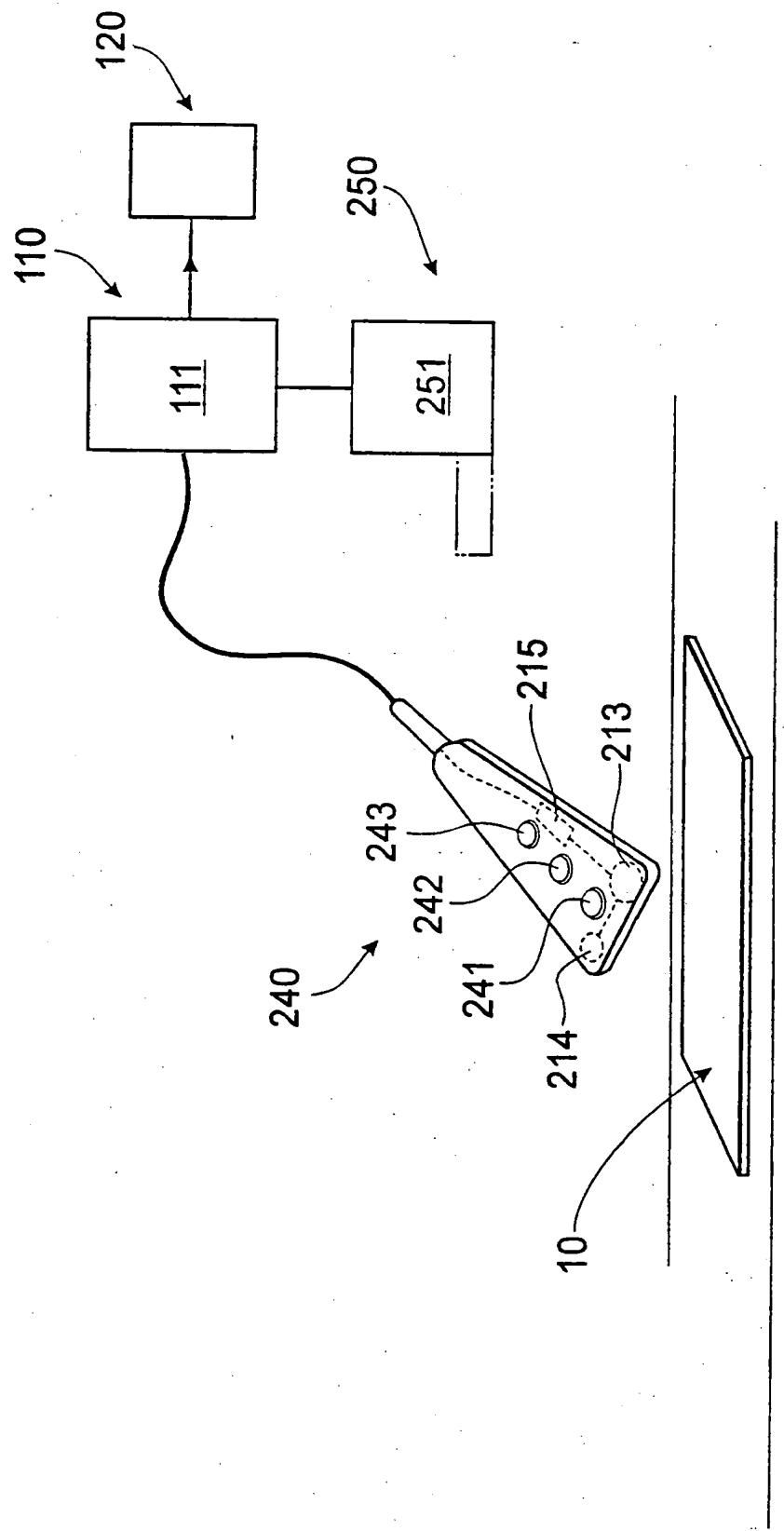


FIG. 5

6 / 7

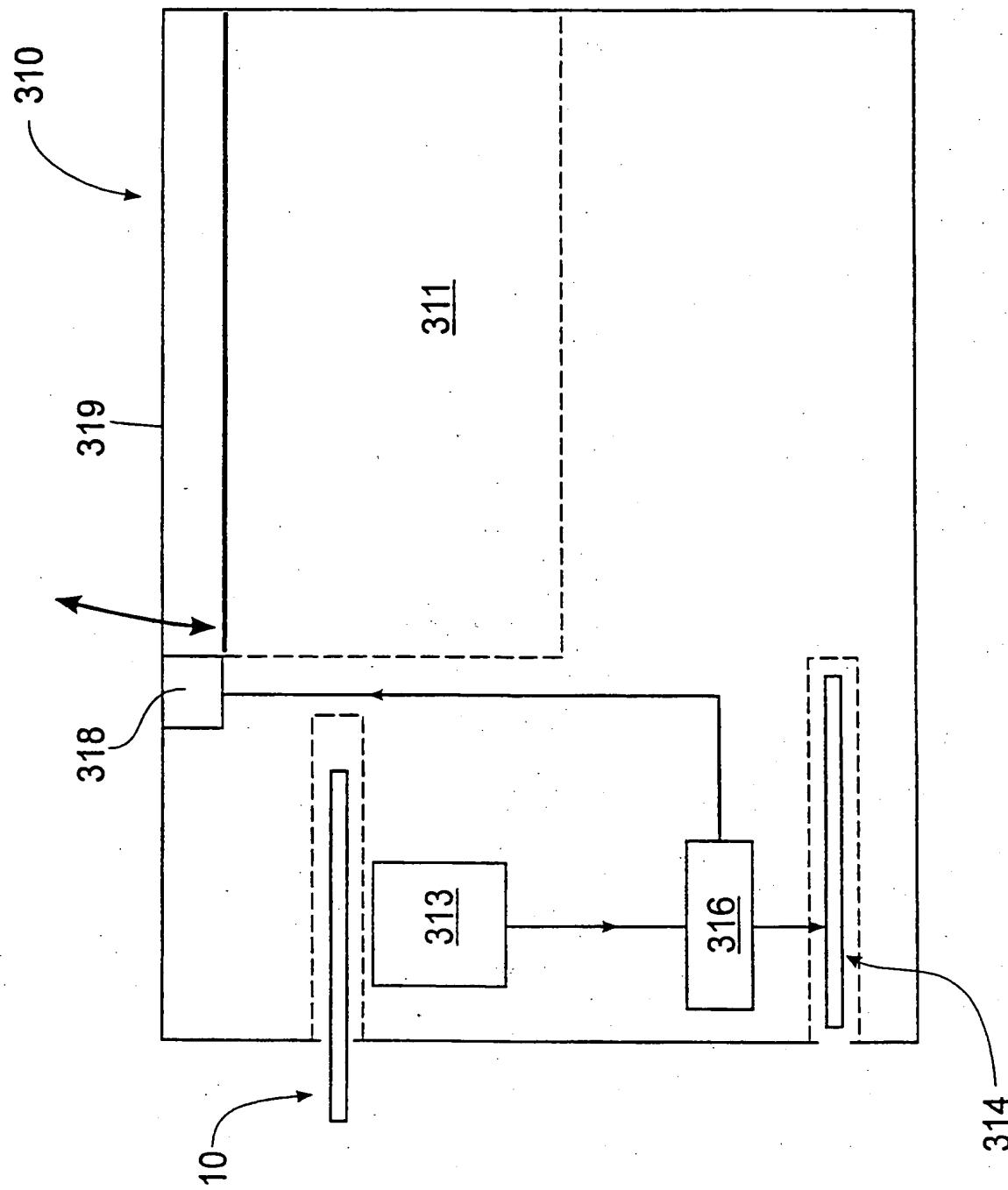


FIG. 6

7 / 7

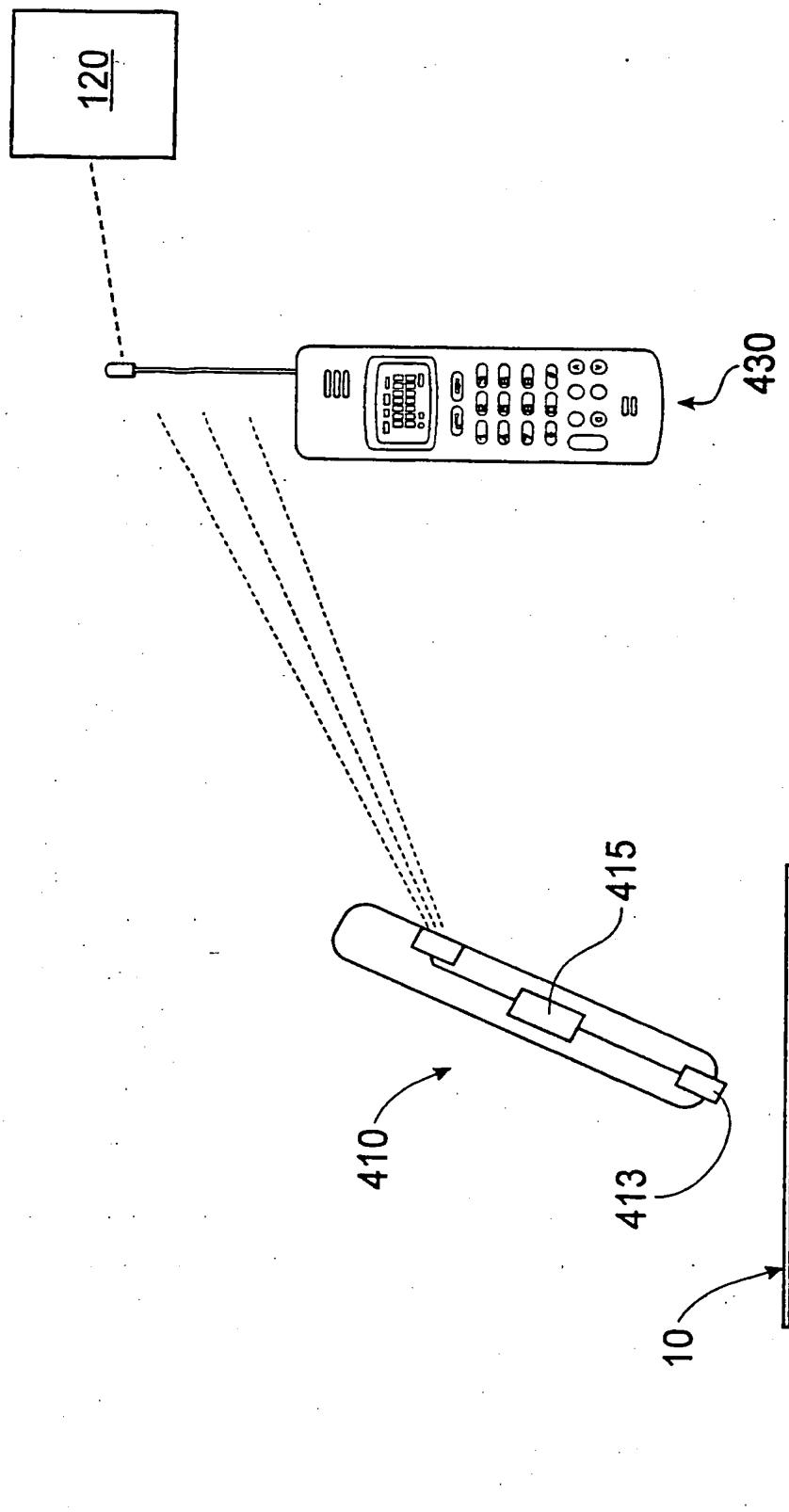


FIG. 7

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/AU00/01081

## A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. <sup>7</sup>: G07D 7/00, 7/20, G07D 11/00, E05G 1/02

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
WPAT, USPTO Web Patent Database, Esp@cenet, "document, banknote, currency, genuine, authentic, database, compare, wallet, purse, safe, scan, card etc"

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 5818021 (SZEWCZYKOWSKI) 6 October 1998 Entire document.	1-12
X	WO, A, 99/04364 (ASSURE SYSTEMS, INC) 28 January 1999 Entire document.	1-12
X	US, A, 5895073 (MOORE) 20 April 1999 Entire document.	1-12
X	US, A, 5790245 (KANESASHI) 4 August 1998 Entire document.	1-12
A	FR, A, 2605674 (VAUTHERIN) 29 April 1988 Entire document.	13

Further documents are listed in the continuation of Box C     See patent family annex

* Special categories of cited documents:		
"A" Document defining the general state of the art which is not considered to be of particular relevance	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent but published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means		
"P" document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search  
7 November 2000

Date of mailing of the international search report  
16 NOV 2000

Name and mailing address of the ISA/AU  
AUSTRALIAN PATENT OFFICE  
PO BOX 200, WODEN ACT 2606, AUSTRALIA  
E-mail address: pct@ipaaustralia.gov.au  
Facsimile No. (02) 6285 3929

Authorized officer  
**P. THONG**  
Telephone No : (02) 6283 2128

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
**PCT/AU00/01081**

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report				Patent Family Member			
US	5818021	WO	98/25212	US	6039249		
WO	99/04364	AU	85778/98	EP	996928		
US	5895073	US	5917925	CA	2192745	GB	2312307
US	5790245	JP	8305922	KR	205778		

**END OF ANNEX**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU00/01081

**Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos :  
because they relate to subject matter not required to be searched by this Authority, namely:
  
  
  
  
2.  Claims Nos :  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
  
  
  
3.  Claims Nos :  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

**Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

- (1) Claims 1-12. Document authentication method or device.
- (2) Claim 13. Document receptacle not requiring the same authentication method or device.

1.  As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims
2.  As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3.  As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
  
  
  
4.  No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

The additional search fees were accompanied by the applicant's protest.  
 No protest accompanied the payment of additional search fees.